

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

-----X	
UNITED STATES OF AMERICA	:
	:
- v -	:
	:
PIERRE GIRGIS,	:
	:
Defendant.	:
-----X	

22 Cr. 6 (KPF)

**DEFENDANT PIERRE GIRGIS'S MOTION
TO COMPEL DISCOVERY**

ANDREW J. DALACK
HANNAH MCCREA
MICHAEL ARTHUS
Federal Defenders of New York, Inc.
Attorneys for Defendant
52 Duane Street, 10th Floor
New York, New York 10007
(212) 417-8700

TO: DAMIAN WILLIAMS
United States Attorney
Southern District of New York
One St. Andrew's Plaza
New York, New York 10007
Attn: AUSAs Kyle Wirshba and Elinor Tarlow

TABLE OF CONTENTS

TABLE OF AUTHORITIES.....	ii
INTRODUCTION.....	1
FACTUAL BACKGROUND.....	2
ARGUMENT.....	8
I. The Court should order the government to disclose the FISA warrants, applications, and related materials.....	9
<i>A. FISA’s background and structure.</i>	10
<i>B. Disclosure and defense participation is necessary to make an accurate determination of the legality of the surveillance and searches.</i>	12
<i>C. If the Court determines that FISA’s statutory rules bar disclosure, the Court should rule that FISA is unconstitutional as applied to this case....</i>	21
<i>D. In addition to disclosing the FISA materials, the Court should order the government to provide notice of any other surreptitious surveillance methods it utilized.</i>	24
II. Under Brady and Rule 16, the government must disclose information (1) material to Mr. Girgis’s <i>Franks</i> motion, (2) material to his <i>mens rea</i> -related defense, and (3) material to undermining the adequacy and good faith of the government’s investigation.	32
<i>A. The government must provide further information about potential misrepresentations or omissions in the traditional search warrant application the government submitted.</i>	33
<i>B. The government must provide information and unredacted reports about the efforts of nine Egyptian officials to turn expatriates into unwitting intelligence assets.</i>	35
<i>C. The Court should order disclosure of information about the role Charles McGonigal played in the Girgis investigation.</i>	38
CONCLUSION	42

TABLE OF AUTHORITIES

Cases

<i>Alderman v. United States</i> , 394 U.S. 165 (1969)	16, 22, 28
<i>Berger v. New York</i> , 388 U.S. 41 (1967).....	27
<i>Biles v. United States</i> , 101 A.3d 1012 (D.C. 2014)	34
<i>Brady v. Maryland</i> , 373 U.S. 83 (1963)	4, 7, 32
<i>Franks v. Delaware</i> , 438 U.S. 154 (1978).....	13
<i>Giglio v. United States</i> , 405 U.S. 150 (1972).....	32
<i>In re All Matters Submitted to the Foreign Intelligence Surveillance Court</i> , 218 F. Supp. 2d 611 (FISA Ct. 2002)	15
<i>In re Grand Jury Matter</i> , 683 F.2d 66 (3d Cir. 1982)	29
<i>In re Kevork</i> , 788 F.2d 566 (9th Cir. 1986)	10
<i>John Doe, Inc. v. Mukasey</i> , 549 F.3d 861 (2d Cir. 2008)	26
<i>Kyles v. Whitley</i> , 514 U.S. 419 (1995).....	32, 40, 41
<i>Nuckols v. Gibson</i> , 233 F.3d 1261 (10th Cir. 2000)	40
<div style="background-color: black; height: 15px; width: 100%;"></div>	
<i>Smith v. Black</i> , 904 F.2d 950 (5th Cir. 1990)	21, 27, 32
<i>United States v. Abubamra</i> , 389 F.3d 309 (2d Cir. 2004)	31
<i>United States v. Abu-Jibaad</i> , 630 F.3d 102 (2d Cir. 2010)	14, 19
<i>United States v. Alter</i> , 482 F.2d 1016 (9th Cir. 1973).....	30
<i>United States v. Apple</i> , 915 F.2d 899 (4th Cir. 1990).....	29
<i>United States v. Arroyo-Angulo</i> , 580 F.2d 1137, 1141 (2d Cir. 1978)	24
<i>United States v. Aziz</i> , 228 F. Supp. 3d 363 (M.D. Pa. 2017)	16
<i>United States v. Belfield</i> , 692 F.2d 141 (D.C. Cir. 1982)	15
<i>United States v. Dalia</i> , 441 U.S. 238 (1979).....	27
<i>United States v. Daoud</i> , 755 F.3d 479 (7th Cir. 2014)	17
<i>United States v. Donovan</i> , 429 U.S. 413 (1977)	27
<i>United States v. Dumeisi</i> , 424 F.3d 566 (7th Cir. 2005)	23
<i>United States v. Duran</i> , 596 F.3d 1283 (11th Cir. 2010)	37
<i>United States v. Elshianway</i> , No. 16-CR-0009, 2017 WL 1048210 (D. Md. Mar. 20, 2017)	10
<i>United States v. Freitas</i> , 800 F.2d 1451 (9th Cir. 1986)	27
<i>United States v. Gamez-Orduno</i> , 235 F.3d 453 (9th Cir. 2000)	21, 32, 35
<i>United States v. Kleinman</i> , 880 F.3d 1020 (9th Cir. 2017)	13
<i>United States v. O'Hara</i> , 301 F.3d 563 (7th Cir. 2002)	23
<i>United States v. Pacella</i> , 622 F.2d 640 (2d Cir. 1980).....	29
<i>United States v. Poindexter</i> , 732 F. Supp. 142 (D.C. 1990)	23
<i>United States v. Rajaratnam</i> , 719 F.3d 139 (2d Cir. 2013)	13
<i>United States v. Stevens</i> , 985 F.2d 1175 (2d Cir. 1993)	33

<i>United States v. Tucker</i> , 526 F.2d 279 (5th Cir. 1976)	29
---	----

Statutes

18 U.S.C. § 3504	28
18 U.S.C. § 951.....	37
18a U.S.C. § 2.....	24
50 U.S.C. § 1801	12, 17
50 U.S.C. § 1804	10, 18, 19
50 U.S.C. § 1805	passim
50 U.S.C. § 1806	passim
50 U.S.C. § 1821	12, 19
50 U.S.C. § 1823	10, 18, 19
50 U.S.C. § 1824	10, 11, 17, 20
50 U.S.C. § 1825	12, 15, 21, 28
50 U.S.C. § 1842	28
50 U.S.C. § 1881a.....	25
50 U.S.C. § 1881e.....	25

Other Authorities

Amos Toh, Faiza Patel, & Elizabeth Goitein, <i>Overseas Surveillance in an Interconnected World</i> , Brennan Center (Mar. 16, 2016)	25
Charlie Savage, <i>Door May Open for Challenge to Secret Wiretaps</i> , N.Y. Times (Oct. 16, 2013)	25
Charlie Savage, <i>Power Wars: Inside Obama's Post-9/11 Presidency</i> (2015)	26
Charlie Savage, <i>Reagan-Era Order on Surveillance Violates Rights, Says Departing Aide</i> , N.Y. Times (Aug. 13, 2014)	28
David S. Kris & J. Douglas Wilson, Nat'l Sec. Investigations & Prosecutions (2012).....	26
Executive Order 12,333.....	25
Jenna McLaughlin, <i>FBI Kept Demanding Email Records Despite DOJ Saying It Needed a Warrant</i> , The Intercept (June 2, 2016)	26
Michael Rothfeld et. al, <i>How Prosecutors Say a Top FBI Agent Sold His Services Overseas</i> , N.Y. Times (Feb. 3, 2023).....	39
NSA Overview of Signals Intelligence Authorities (Jan. 8, 2007)	25
S. Rep. No. 1097	28
S. Rep. No. 95–701.....	16
S. Rep. No. 96-823	23

Rules

Fed. R. Crim. P. 16.....	passim
--------------------------	--------

Regulations

3 C.F.R. § 202, 210-12 (1981)	25
-------------------------------------	----

INTRODUCTION

Defendant Pierre Girgis moves to compel discovery of: (1) all FISA warrants, applications, and materials related to his case; (2) notice of all surreptitious government surveillance of his communications and personal information; (3) all information in the government's control regarding potential material misrepresentations and omissions in the government's warrant applications; (4) any information in the government's possession regarding the efforts of nine Egyptians, all identified as having relationships with Mr. Girgis, to "turn" expatriates into unwitting assets; and (5) all information in the government's possession about the role of disgraced former FBI Special Agent in Charge Charles McGonigal in the investigation of this case. Disclosure of this information is necessary so that the defense can:

- Challenge, through an adversarial process, the legality of the FISA surveillance and any other surreptitious surveillance the government may have employed;
- Effectively litigate motions to suppress, including *Franks* issues that are apparent from the face of the discovery the government has provided;
- Prepare a defense related to Mr. Girgis's lack of *mens rea*; and
- Challenge the adequacy, reliability, and good faith of the government's investigation.

This motion is based on the Fourth, Fifth, and Sixth Amendments to the United States Constitution; the Foreign Intelligence Surveillance Act; Federal Rule of Criminal Procedure 16; and 18 U.S.C. § 3504.

FACTUAL BACKGROUND

On January 5, 2022, the government indicted United States citizen Pierre Girgis on charges that he violated the Foreign Agents Registration Act (“FARA”) by acting as an agent of the Egyptian government without notifying the Attorney General. 18 U.S.C. §§ 371, 951. A few weeks later, the government filed a boilerplate notice of its intent to use “information obtained or derived from electronic surveillance and physical search conducted pursuant to the Foreign Intelligence Surveillance Act of 1978 (FISA).” FISA Notice, ECF No. 11. It did not provide any further details about the FISA surveillance conducted in this case; did not disclose the FISA applications, warrants, or related materials; and did not reveal whether it had engaged in any other surreptitious surveillance of Mr. Girgis’s electronic or telephonic communications.

The government’s ensuing discovery productions revealed that Mr. Girgis had been the target of wide-ranging electronic surveillance. The government turned over hundreds of recorded phone calls, thousands of electronic messages, and FBI reports indicating that Mr. Girgis had been under investigation for years. Yet the government never produced the underlying FISA materials, and many of the FBI reports it disclosed – including those related to alleged Egyptian officials who “tasked” Mr. Girgis – were heavily redacted.

On June 2, 2022, the government made a *Brady* disclosure. The government revealed that FBI Special Agent Brian Connors – who was the affiant on FISA applications and a 2019 traditional search warrant application – had access to

information as early as May 2018 that one of his key sources for an application to search Mr. Girgis’s electronic devices and online accounts, [REDACTED], had been “fired for improperly involving himself in throwing out a case.” Ex. A.¹ The government included notes showing that [REDACTED] was convicted of conspiracy and official misconduct in a case that received press coverage in 2017; Connors knew [REDACTED] “had criminal history of some sort,” but never conducted a standard background check before utilizing [REDACTED]; Connors was repeatedly alerted to the existence of [REDACTED] criminal history but never looked into it; Connors may not have officially signed [REDACTED] up as a confidential human source; and Connors failed to include any information about [REDACTED] criminal history in his search warrant affidavits. *Id.* Indeed, in the 2019 traditional search warrant application for Mr. Girgis’s electronic devices and online accounts – to date, the only warrant application the government has disclosed – Connors merely referred to [REDACTED] as “Retired Captain-1.” Ex. B (emphasis added).

Separate from the *Brady* disclosure, the government provided an email Connors sent to AUSA Kyle Wirshba, dated June 23, 2020, with the subject line “Update”:

¹ [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

[REDACTED]

[REDACTED]
[REDACTED] [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

[REDACTED]

Ex. C. The government did not specify what the “misstatement/omission” was, or why it was determined not to rise to the level of materiality.

By a letter dated October 20, 2022, the defense requested, in relevant part, disclosure of the following items, pursuant to Fed. R. Crim. P. 16 and *Brady v. Maryland*, 373 U.S. 83 (1963):

1. Unredacted copies of certain Confidential Human Source Reports and Electronic Communications containing information about certain Egyptian officials. These items were identified as material to the preparation of Mr. Girgis’s defense: “that certain Egyptian officials intended to manipulate [him] and ‘turn’ him into an unwitting stooge.” [Request 1a].
2. Unredacted reports and further information in the government’s possession regarding the potential misstatement or omission referenced in the June 23, 2020, email, and why it was determined not to rise to the level of materiality. [Request 1b].
3. Unredacted copies of four reports detailing certain relevant aspects of the FBI’s investigation into Mr. Girgis. [Requests 1f-1i].
4. Two unredacted reports, as well as information in the government’s possession, regarding nine purported

Egyptian officials named in FBI reports: [REDACTED]
 [REDACTED]
 [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]
 [REDACTED]. The defense specifically requested information about these individuals' relationships with Mr. Girgis, [REDACTED], or the Egyptian government.[Requests 1c-1d, 3a-3i].

Ex. D.

After the defense sent that discovery request, the Justice Department unsealed two indictments charging Charles McGonigal, former Special Agent in Charge of the FBI's New York Counterintelligence Division, with money laundering, conspiring to evade sanctions, and concealing payments from foreign sources. In the Southern District of New York, prosecutors alleged that McGonigal, before he retired from the FBI in 2018, formed a relationship with a representative of sanctioned Russian oligarch Oleg Deripaska. Following his retirement, prosecutors alleged that McGonigal investigated a rival of Deripaska in exchange for concealed payments. Ex. J. Meanwhile, in the District of Columbia, the government alleged that, while still at the FBI, McGonigal received payments from a former Albanian intelligence agent and was introduced to the Albanian Prime Minister. McGonigal subsequently opened an official investigation into a United States citizen who belonged to a rival political party of the Prime Minister, during which the intelligence agent acted as a confidential human source. Ex. K. The criminal behavior alleged in the indictments occurred while McGonigal was leading the Counterintelligence Division investigating Mr. Girgis – an investigation that utilized foreign-born sources and implicated the tension between the

Egyptian Muslim Brotherhood and the regime of Egyptian President Abdelfattah El-Sisi.

Upon learning of the indictments against McGonigal, the defense sent a follow-up discovery request to the government on February 6, 2023, seeking disclosure of any and all information regarding McGonigal's involvement in the Girgis investigation. Ex. G.

The government responded to both discovery requests on March 2, 2023. It removed a few minor redactions from its previous materials and provided some new documents. But it refused to provide most of the information the defense sought, insisting it was not discoverable:

1. Regarding the request for unredacted confidential human source reports [Request 1a], the government asserted that it would not disclose information not directly "relating to the defendant or his statements."
2. Regarding information about the potential material misrepresentation and omissions in Connors's warrant applications [Request 1b], the government removed minor redactions from some documents and clarified that the email about a potential misstatement referred to Connors.
3. Regarding the remaining unredacted reports the defense requested [Requests 1c-1d, 1f-1i], the government indicated that it had turned over portions relevant to Connors's warrant applications, but believed the remaining request for information was overbroad or the materials were not discoverable.

Regarding the requests for information about named Egyptian officials [Request 3] and McGonigal, the

government asked for further information about why the defense believed the materials were discoverable.

Ex. H.

The defense wrote to the government on March 20, 2023. It clarified that Mr. Girgis was preparing a defense that, at most, he was the target of a campaign by Egyptian authorities to turn him into an unwitting intelligence asset. Therefore, information about the nine Egyptians' efforts to engage in "operations aimed at cultivating unwitting assets," is material to his defense and discoverable under Fed. R. Crim. P. 16 and *Brady*. Likewise, since McGonigal was in charge of the FBI Counterintelligence Division at the time it was investigating Mr. Girgis, McGonigal was accused of concealing payments from sources in exchange for investigations, and the Girgis investigation involved the mishandling of sources, the defense was "entitled to information regarding whether McGonigal oversaw or was involved in any part of the investigation into Mr. Girgis, authorized any steps in that investigation, and/or approved any classified FISA warrant applications." Ex. I.

During a phone conversation on March 23, 2023, the government indicated that it would not provide any further information about the nine Egyptian officials or McGonigal. The government insisted that information about the Egyptian officials was not relevant to any elements of the charged crimes, and that information about McGonigal's role in the investigation was not discoverable.

ARGUMENT

The government has served notice of its intent to use evidence obtained or derived from FISA surveillance. Yet it has failed to turn over any of the FISA warrants, applications, or related materials. Nor has the government disclosed whether it used and/or relied upon any other surreptitious surveillance methods to investigate Mr. Girgis and intercept his electronic and telephonic communications. As a result, it is practically impossible for the defense to make informed suppression arguments and provide critical input on the complex statutory and constitutional issues the Court will be tasked with resolving.

What the government has revealed, however, is that the affiant on the FISA and traditional search warrant applications, Special Agent Brian Connors, omitted critical information from those applications regarding the suspect credibility of his chief source. And based on an email the government has turned over, it appears that Connors and another government official reviewed Connors's warrant applications (traditional and FISA) and determined that "it" did not "reach the level of material misstatement/omission." But the government has not explained what "it" referred to, and has not further explained why it believes Connors's misstatements and/or omissions are immaterial. The defense requires additional discovery in order to mount an effective *Franks* challenge to both the FISA and traditional search warrants.

Making matters worse, the government has refused to provide several items of discovery that are material to Mr. Girgis's defense. The government refuses to disclose

information about the efforts of nine specified Egyptians to conduct a campaign to recruit unwitting foreign assets in the United States – even though the discovery suggests that those same Egyptians were seeking to recruit and “task” Mr. Girgis. And the government is unwilling to provide information about the role former FBI Special Agent in Charge of Counterintelligence Charles McGonigal played in the Girgis investigation – even though McGonigal has been indicted for accepting concealed payments from foreign agents to investigate their political rivals during the time period when McGonigal’s Counterintelligence Division was investigating Mr. Girgis. The defense remains in the dark about the genesis of the investigation into Mr. Girgis, but would plainly be entitled to any information suggesting that the investigation into him was motivated by any payments or remunerations to McGonigal by foreign agents or their affiliates.

The materials and information the defense seeks are plainly discoverable under the Constitution, statutory law, and Federal Rule of Criminal Procedure 16. Therefore, the Court should order the government to disclose the requested discovery.

I. The Court should order the government to disclose the FISA warrants, applications, and related materials.

The government has served notice that it intends to introduce evidence obtained or derived from FISA surveillance. Given that notice and the remarkable volume of Mr. Girgis’s communications that the government has provided as part of Rule 16 discovery, it is clear that Mr. Girgis was the target of FISA surveillance and/or that his

communications were intercepted incidentally to the government’s surveillance of other individuals.

The defense intends to file a motion to suppress the FISA-derived evidence. But the defense cannot effectively litigate a suppression motion – particularly one raising complex statutory issues and a fact-specific *Franks* claim – without being permitted to see the warrant materials or participate in an adversarial process. Accordingly, the Court should order disclosure of the FISA warrants, applications, and related materials.

A. FISA’s background and structure.

Enacted in 1978, the Foreign Intelligence Surveillance Act (“FISA”) was intended to balance civil liberties against the government’s desire to gather foreign intelligence. *See In re Kevork*, 788 F.2d 566, 569 (9th Cir. 1986). Among other provisions, FISA established a secret court, the Foreign Intelligence Surveillance Court (“FISC”), in which only the government is permitted to appear. At the FISC, the government can seek warrants authorizing extensive electronic surveillance and physical searches of United States citizens. *See United States v. Elshianway*, No. 16-CR-0009, 2017 WL 1048210, at *3 (D. Md. Mar. 20, 2017).

To obtain a FISA warrant, the government must submit an application containing a federal officer’s sworn affidavit. 50 U.S.C. §§ 1804-1805, 1823-1824. Among other things, a FISA application must:

- (1) Demonstrate probable cause to believe that the target is an “agent of a foreign power,” and that the premises to be searched or facility to be surveilled is, or is about to be,

owned or used by an agent of a foreign power. *Id.* §§ 1804(a)(3), 1805(a)(2), 1823(a)(3), 1824(a)(2);

(2) Contain a certification attesting, among other things, that a “significant purpose” of the surveillance or search “is to obtain foreign intelligence information,” and that “such information cannot reasonably be obtained by normal investigative techniques.” *Id.* §§ 1804(a)(6)(B)-(C), 1805(a)(4), 1823(a)(6)(B)-(C), 1824(a)(4); and

(3) Establish minimization procedures that are designed to limit the “acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons.” *Id.* §§ 1801(h), 1804(a)(4), 1805(a)(3), 1821(4), 1823(a)(4), 1824(a)(3).

In reviewing an application to surveil or search a United States citizen, the FISC must ensure that probable cause is not based “solely upon the basis of activities protected by the [F]irst [A]mendment.” *Id.* §§ 1805(a)(2)(A), 1824(a)(2)(A).

FISA warrants issued against United States citizens only last for 90 days. *Id.* §§ 1805(d)(1), 1824(d)(1). After that period has passed, the government must return to the FISC to seek extensions. Such extension requests must be accompanied by an application, and the FISC must make new findings. *Id.* §§ 1805(d)(2), 1824(d)(2).

Although FISA surveillance is conducted in secret, the government is not entitled to hide FISA-derived information from criminal defendants. Rather, if the government intends to use information obtained or derived from FISA surveillance in a criminal case, it must give notice to the “aggrieved person” – either the target of surveillance or a search, or anyone whose “communications or activities were subject to electronic

surveillance” or whose “premises, property, information, or material was subject to physical search.” *Id.* §§ 1801(k), 1806(c), 1821(2), 1825(d). That person can then move to suppress the evidence on the grounds that “the information was unlawfully acquired” or that the surveillance or search “was not made in conformity with an order of authorization or approval.” *Id.* §§ 1806(e), 1825(f). After the filing of a suppression motion, the Attorney General may file an affidavit claiming that disclosure or an adversary hearing would harm national security. The District Court must then review “in camera and ex parte the application, order, and such other materials” relating to the search or surveillance “as may be necessary to determine whether” the surveillance or search “was lawfully authorized and conducted.” *Id.* §§ 1806(f), 1825(g).

The filing of the Attorney General’s affidavit does not, however, cut the defense out of the picture. When “necessary to make an accurate determination of the legality” of the surveillance or search, the court “may disclose to the aggrieved person, under appropriate security procedures and protective orders, portions of the application, order, or other materials,” or “may require the Attorney General to provide to the aggrieved person a summary of such materials.” *Id.* And even if the court determines that the surveillance or search was lawful, it may nevertheless order disclosure of the FISA materials “to the extent that due process requires.” *Id.* §§ 1806(g), 1825(h).

B. Disclosure and defense participation is necessary to make an accurate determination of the legality of the surveillance and searches.

1. Disclosure is necessary so the defense can meaningfully litigate an apparent *Franks* issue.

A warrant issued based on lies and omissions cannot comport with the Fourth Amendment. The Supreme Court has held that when a defendant makes a “substantial preliminary showing that a false statement knowingly and intentionally, or with reckless disregard for the truth, was included by the affiant in the warrant affidavit, and if the allegedly false statement is necessary to the finding of probable cause, the Fourth Amendment requires that a hearing be held at the defendant’s request.” *Franks v. Delaware*, 438 U.S. 154, 155-56 (1978). A *Franks* hearing is thus mandated when a warrant affidavit contains statements that are affirmatively false, or when it contains material omissions that, had they been included, would have undermined the probable cause determination. See *United States v. Kleinman*, 880 F.3d 1020, 1038 (9th Cir. 2017) (omissions are material when there would not be probable cause had the information been included in the warrant application); *United States v. Rajaratnam*, 719 F.3d 139, 154-55 (2d Cir. 2013) (although not automatic, the omission of critical evidence from a warrant application can give rise to inference of reckless disregard for the truth under *Franks*).

FISA warrants, particularly those targeting United States citizens, are not exempt from the Fourth Amendment. Rather, given the secret, *ex parte* nature of the FISA process, it is even more important that FISA applications contain an honest and complete disclosure of all the relevant facts. Therefore, as with any other warrant, FISA

warrants are subject to challenge on *Franks* grounds. See *United States v. Abu-Jihaad*, 630 F.3d 102, 130-31 (2d Cir. 2010).

The defense anticipates raising a *Franks* claim with regard to the FISA motions in Mr. Girgis's case.² Based on the government's discovery and *Brady* disclosures, Special Agent Brian Connors – who identified himself as the affiant in FISA applications related to this case – made misrepresentations and omissions in his warrant affidavits. As early as May 10, 2018, Connors was alerted to the fact that one of his principal sources of information about Mr. Girgis, [REDACTED], had a criminal record. In fact, [REDACTED] had been fired from his job and convicted of official misconduct following a well-publicized incident in which he helped cover up a burglary his friend's son committed. When Connors was interviewed by federal prosecutors in connection with the Girgis information, he claimed he did not conduct a standard background check despite repeatedly hearing about [REDACTED] checkered past, and admitted he did not include any information about [REDACTED] crimes in his search warrant affidavits. Ex. A.

The information in the government's *Brady* disclosure gives rise to a colorable – and quite strong – *Franks* claim, with respect to both the FISA and traditional warrants. Indeed, in a traditional warrant application Connors submitted in 2019, he referred to

² The defense is not asking the Court to rule on the *Franks* claim, or any other suppression claims, at this time. This motion is addressed only toward compelling discovery, so that the defense can make an effective and informed suppression motion at the Rule 12 stage.

██████ as “*Retired* Captain-1,” without noting that ██████ “retirement” was in fact a firing for official misconduct. Ex. B (emphasis added). That Connors so brazenly created a *Franks* issue with his material misstatements in the traditional search warrant application strongly indicates the existence of a *Franks* claim as to the FISA warrant applications. And the troubling nature of Connors’s flawed warrant applications was not lost on the government: Connors himself discussed his warrant applications with someone named ██████ whose “chain” apparently reviewed Connors’s affidavits to determine if an unspecified “it” reached “the level of material misstatement/omission.” Ex. C. The fact that the government was apparently concerned that Connors’s other warrant affidavits were tainted creates a compelling inference that his FISA warrant applications were defective on *Franks* grounds.

Although the information the government has provided points to the *existence* of a *Franks* claim, the defense cannot effectively *litigate* that issue without access to the FISA materials.³ Indeed, *Franks* claims like the one presented here are precisely the kinds of situations where “disclosure is necessary to make an accurate determination of the legality of the” FISA warrants. 50 U.S.C. § 1806(f), 1825(g); see *United States v. Belfield*, 692 F.2d 141, 147 (D.C. Cir. 1982) (recognizing that Congress intended that courts

³ This would not be the first time a FISA warrant resulted from a *Franks* violation. In other cases, the government has conceded making “misstatements and omissions of material facts” in FISA applications. See *In re All Matters Submitted to the Foreign Intelligence Surveillance Court*, 218 F. Supp. 2d 611, 620-21 (FISA Ct. 2002).

order disclosure where “the court’s initial review of the application, order, and fruits of the surveillance indicates that the question of legality may be complicated by factors such as ‘indications of possible misrepresentation of fact’”) (quoting S. Rep. No. 95–701). The government has turned over nearly 200,000 pages of discovery (albeit heavily redacted), including countless FBI reports referring to [REDACTED], hundreds of phone calls in Egyptian Arabic, and thousands of intercepted electronic messages, spanning years of investigation that Connors principally conducted. Given the volume of information at issue, the Court simply cannot identify what misstatements or omissions Connors made, let alone whether they were material to the probable cause determination, without defense input. Endeavoring to do so *ex parte*, without adversarial litigation, would violate not only FISA but also the Due Process Clause. *Alderman v. United States*, 394 U.S. 165, 183-84 (1969) (the “superiority” of adversary proceedings is “nowhere more evident than in those cases . . . where an issue must be decided on the basis of a large volume of factual materials, and after consideration of the many and subtle interrelationships which may exist among the facts reflected by these records”).

Without access to the FISA materials, the defense “must endeavor to establish the falsity of statements that the law does not allow [it] to see.” *United States v. Aziz*, 228 F. Supp. 3d 363, 371 (M.D. Pa. 2017). Put differently, “the secrecy shrouding the FISA process” can render it “impossible for a defendant to meaningfully obtain relief under *Franks*” – relief Mr. Girgis is constitutionally entitled to pursue. *United States v.*

Daoud, 755 F.3d 479, 485-86 (7th Cir. 2014) (Rovner, J. concurring). Denying the defense the opportunity to review the FISA materials in a case like Mr. Girgis’s would thus violate not only FISA but also the Fourth, Fifth, and Sixth Amendments. The Court should order disclosure of the FISA warrants, applications, and related materials.

2. Disclosure is necessary for the defense to litigate the other FISA-related suppression issues presented in this case.

In addition to the *Franks* claim discussed above, the defense anticipates raising a number of other challenges to the legality of the FISA warrants. Disclosure of the FISA materials is necessary for the defense to provide the input the Court will need to accurately determine these issues.

First, the Court will need to decide whether the FISA applications established probable cause to believe that Mr. Girgis was an “agent of a foreign power,” and that the premises to be searched or surveilled were being used or were about to be used by a foreign power or agent. 50 U.S.C. §§ 1805(a)(2), 1824(a)(2). This will require an analysis of the complicated question of whether there was a reasonable probability Mr. Girgis qualified as an “agent of a foreign power” at the time the FISA surveillance began: that is, someone who knowingly engaged in clandestine intelligence gathering activities on behalf of a foreign power in a manner violative of the criminal laws of the United States. 50 U.S.C. § 1801(b)(2)(A)-(B). And since Mr. Girgis is a United States citizen, ruling on the issue will require the Court to resolve the difficult issue of whether Mr. Girgis was targeted “solely upon the basis of activities protected by the [F]irst

[A]mendment.” 50 U.S.C. § 1805(a)(2)(A). Indeed, there is no allegation or evidence that Mr. Girgis received any benefits or remunerations of any kind for his alleged “work” on behalf of the Egyptian government, nor is there any suggestion that he had an employer-employee relationship of any kind with any Egyptian government agency. Instead, the government’s allegations against Mr. Girgis turn entirely on his alleged attempts to organize large trips to Egypt and arrange meetings of various kinds, distribute information, express support for certain groups, and converse with various individuals. Accordingly, whether Mr. Girgis’s activities were protected by the First Amendment is a complicated question that demands defense input. Without being able to see the allegations the government included in the FISA applications, however, the defense cannot meaningfully litigate these issues.

Second, Mr. Girgis’s case will present difficult questions about the necessity of the government’s use of the FISA process. A FISA warrant may only be issued when the Attorney General certifies “that such information cannot reasonably be obtained by normal investigative procedures.” 50 U.S.C. §§ 1804(a)(6)(C), 1823(a)(6)(C). Here, however, it appears the government also obtained evidence using traditional search warrants, subpoenas, and information (including clandestine recordings) that came from confidential human sources. The Court’s determination of the need for FISA surveillance can only meaningfully occur if the defense has the opportunity to review the FISA materials, evaluate the adequacy of the government’s certifications in the

context of the hundreds of thousands of pages of discovery that have been produced, and present adversarial arguments.

Third, the forthcoming suppression motion will raise tough questions about whether the collection of foreign intelligence information was a “significant purpose” of the FISA applications. 50 U.S.C. §§ 1804(a)(6)(A)-(B), 1823(a)(6)(A)-(B). In seeking a FISA warrant, the government must “have a measurable foreign intelligence purpose, other than just criminal prosecution of even foreign intelligence crimes.” *Abu-Jihaad*, 630 F.3d at 128. The discovery provided thus far raises the distinct possibility that the FISA applications here were substantially motivated by the goal of prosecuting Mr. Girgis. That is precisely the type of issue that demands defense input and adversarial litigation.

Fourth, this case raises serious minimization concerns. Minimization procedures must be, among other things, “reasonably designed in light of the purpose and technique of the particular” search or surveillance “to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information.” 50 U.S.C. §§ 1801(h)(1), 1821(4). Here, however, the government intercepted thousands of messages and hundreds of phone calls from Mr. Girgis, spanning several years and at least two continents. Given the sheer breadth of the communications that were intercepted, there is a serious question whether the government designed adequate

minimization procedures or actually followed them. The Court should order the FISA materials disclosed so that the defense can evaluate and meaningfully challenge the government's minimization procedures.

And fifth, the sheer length of the government's surveillance of Mr. Girgis will present a potential basis for suppression. Based on the (heavily redacted) discovery provided, it appears that the government intercepted and surveilled Mr. Girgis's communications for several years. Under 50 U.S.C. §§ 1805(d) and 1824(d), however, a FISA warrant must be renewed every 90 days. The defense should therefore be provided the underlying FISA materials so that it can effectively address whether the government abided by FISA's time limitations, and whether each FISA warrant was issued based on a sufficient (and uncorrupted) application.

The defense cannot effectively litigate these complex questions – and others that will doubtless emerge in the still-secret materials – without a chance to review the FISA warrants, applications, and related documents. And the Court cannot be expected to accurately determine the legality of the FISA warrants without defense input, particularly since this litigation involves placing over 200,000 pages of discovery and hundreds of recorded calls (in Egyptian Arabic) into context. The Court should, therefore, order disclosure.

C. If the Court determines that FISA’s statutory rules bar disclosure, the Court should rule that FISA is unconstitutional as applied to this case.

To satisfy the Fourth, Fifth, and Sixth Amendments, the government must disclose to the defense any information that could affect a suppression ruling. *See, e.g., United States v. Gamez-Orduno*, 235 F.3d 453, 461 (9th Cir. 2000) (“The suppression of material evidence helpful to the accused, whether at trial or on a motion to suppress, violates due process if there is a reasonable probability that, had the evidence been disclosed, the result of the proceeding would have been different”); *Smith v. Black*, 904 F.2d 950, 965-66 (5th Cir. 1990), *vacated on other grounds*, 503 U.S. 930 (1992) (due process mandates the disclosure of information that would “affect[] the outcome of [a] suppression hearing”). Indeed, FISA specifically directs courts to grant a defendant’s motion to compel “to the extent that due process requires discovery or disclosure.” 50 U.S.C. §§ 1806(g); 1825(h).

Yet the government is certain to argue that the Court should deny disclosure and instead review the materials entirely *in camera*. Although FISA permits *in camera* review, the statute’s provisions allowing for determination of a suppression motion without any defense participation whatsoever violate Mr. Girgis’s Fourth, Fifth, and Sixth Amendment rights, particularly given the unique circumstances of his case. Therefore, to the extent the government relies on FISA to insist on *in camera* review, those portions of FISA are unconstitutional.

A court's *ex parte, in camera* review of warrant materials is no substitute for the single-minded advocacy of defense counsel. For that reason, and especially when it comes to complex suppression issues, the Supreme Court has emphasized that adversary procedures are critical to satisfying the Constitution:

[T]he need for adversary inquiry is increased by the complexity of the issues presented for adjudication. . . . Adversary proceedings will not magically eliminate all error, but they will substantially reduce its incidence by guarding against the possibility that the trial judge, through lack of time or unfamiliarity with the information contained in and suggested by the materials, will be unable to provide the scrutiny which the Fourth Amendment exclusionary rule demands.

Alderman, 394 U.S. at 184. The defense perspective is indispensable in cases involving electronic surveillance, since “the volume of the material to be examined and the complexity and difficulty of the judgments involved” demand adversarial litigation. *Id.* at 182 n.14.

FISA, by contrast, permits courts to wholly exclude defense counsel from suppression litigation. It authorizes courts under some circumstances to determine the legality of searches and surveillance without allowing counsel to even see the materials he or she is attempting to challenge. Such a secretive, one-sided procedure violates core components of due process, the exclusionary rule, the right to be present, and the right to the effective assistance of counsel. This is particularly true in the case of Mr. Girgis – a United States citizen whose communications were intercepted domestically, and who enjoys the full range of protections afforded by the Fourth, Fifth, and Sixth

Amendments. Especially in light of Connors’s documented issues with misstatements and/or omissions in warrant affidavits in this case, adversarial proceedings are especially crucial here.

The mere fact that the FISA materials may be “classified” does not change the analysis.⁴ The classification status of the requested materials is relevant to a ruling under CIPA – a procedural statute that cannot displace a defendant’s Fourth, Fifth, or Sixth Amendment rights. In any event, CIPA’s “fundamental purpose” is “to protect [] and [] restrict the discovery of classified information in a way that does not impair the defendant’s right to a fair trial.” *United States v. Dumeisi*, 424 F.3d 566, 578 (7th Cir. 2005) (quoting *United States v. O’Hara*, 301 F.3d 563, 569 (7th Cir. 2002)). Indeed, CIPA “rests on the presumption that the defendant should not stand in a worse position, because of the fact that classified information is involved, than he would without [CIPA].” S. REP. NO. 96-823, at 9 (1980), *reprinted in* 1980 U.S.C.C.A.N. 4294, 4302. Therefore, to the extent the government may argue that the FISA materials cannot be disclosed because they are “classified,” the proper remedy is to ensure compliance under CIPA, not to withhold the materials from the defense in violation of the Constitution. *See United States v. Poindexter*, 732 F. Supp. 142, 154-55 (D.C. 1990) (to the

⁴As the Court is aware, lead defense counsel for Mr. Girgis, Andrew Dalack, possesses the appropriate security clearances and has substantial experience dealing appropriately with classified discovery. And following discussions with the government about an appropriate classified protective order, the defense would also be willing to accept the requested materials on an “attorney’s eyes only” basis.

extent questioning of the President may elicit national security information, the proper remedy is CIPA compliance).⁵

In sum, disclosure of the FISA materials is required under the Fourth, Fifth, and Sixth Amendments. To the extent FISA may be read otherwise, it is unconstitutional.

D. In addition to disclosing the FISA materials, the Court should order the government to provide notice of any other surreptitious surveillance methods it utilized.

Given the astounding quantity of telephonic and electronic communications the government intercepted from Mr. Girgis – some of which appear to have potentially been intercepted when Mr. Girgis was overseas – and the scope and length of the investigation into Mr. Girgis, the defense has serious concerns that the government may have gone beyond traditional FISA surveillance and utilized other surreptitious surveillance methods. Mr. Girgis cannot meaningfully challenge the lawfulness of any such surveillance and the government’s reliance on it, however, unless the government provides notice of the methods that were actually used. Therefore, the Court should order the government to provide notice of any surreptitious surveillance methods it

⁵ Following the government’s opposition to the present motion and before any defense reply, the defense may seek an *ex parte* conference with the Court pursuant to Section 2 of the Classified Information Procedures Act. *See* 18a U.S.C. § 2 (“At any time after the filing of the indictment or information, any party may move for a pretrial conference to consider matters relating to classified information that may arise in connection with the prosecution”). And while the Court may entertain an *ex parte* application from the government to withhold certain classified materials from discovery (*see* 18a U.S.C. § 4), the Court should decline to receive the entire application *ex parte* and, instead, allow the defense the opportunity to address the government’s legal arguments in support of non-disclosure. Given the unique circumstances of this case, a fully *in camera* and *ex parte* CIPA § 4 proceeding would be “manifestly [] incompatible with our system of criminal jurisprudence.” *United States v. Arroyo-Angulo*, 580 F.2d 1137, 1141 (2d Cir. 1978) (citations omitted).

utilized in this case, including surveillance under Executive Order 12,333, FISA Section 702, or national security letters.

Executive Order 12,333 is the National Security Agency's "primary source" of intelligence gathering and governs most surveillance covered abroad. See NSA Overview of Signals Intelligence Authorities, p. 4 (Jan. 8, 2007), <http://bit.ly/1ruKbBk>; see also 3 C.F.R. § 202, 210-12 (1981), reprinted as amended, note following 50 U.S.C. § 401, pp. 543, 547-48. The NSA utilizes Executive Order 12,333 to collect electronic content and metadata, and uses this information when investigating United States citizens. *See generally* Amos Toh, Faiza Patel, & Elizabeth Goitein, *Overseas Surveillance in an Interconnected World*, Brennan Center (Mar. 16, 2016), <http://bit.ly/1UfSdMW>; *Two Sets of Rules for Surveillance, Within U.S. and on Foreign Soil*, N.Y. Times (Aug. 13, 2014), <http://nyti.ms/1u2juDt> (chart describing uses of E.O. 12,333 surveillance).

FISA Section 702 is another method the government utilizes to surveil United States citizens. Section 702 permits the government to intercept communications when one party to the conversation is a non-U.S. person located overseas, even if the other party is a U.S. citizen on American soil. 50 U.S.C. § 1881a(a). When Section 702 is invoked, the government need not demonstrate that its targets are agents of foreign powers or engaged in criminal activity. Although notice of Section 702 surveillance is statutorily mandated, 50 U.S.C. §§ 1806, 1881e(a), the government has a long track record of narrowly interpreting its notice obligations in this context. *See* Charlie Savage, *Door May Open for Challenge to Secret Wiretaps*, N.Y. Times (Oct. 16, 2013),

<http://nyti.ms/1r7mbDy> (describing how the Justice Department “long used a narrow understanding of what ‘derived from’ means” to improperly withhold notice from criminal defendants); Charlie Savage, *Power Wars: Inside Obama’s Post-9/11 Presidency*, 586-93 (2015) (reporting that the Justice Department is withholding notice based on unilateral determinations that Section 702 surveillance was not “material” or “critical”).

Finally, national security letters are a means by which the government frequently obtains information in national security cases without any judicial review. National security letters require recipients, like electronic service providers, to disclose certain types of customer records. The recipients are typically prohibited from notifying their customers that they received such a demand. David S. Kris & J. Douglas Wilson, Nat’l Sec. Investigations & Prosecutions 728 (2012); *see also John Doe, Inc. v. Mukasey*, 549 F.3d 861, 883 (2d Cir. 2008) (finding gag provisions unconstitutional “to the extent that they impose a nondisclosure requirement without placing on the Government the burden of initiating judicial review of that requirement”). Even after the Justice Department’s Office of Legal Counsel concluded in 2008 that it was unlawful for the FBI to seek certain types of internet records using national security letters, the FBI continued to use such letters to demand that information for years. *See* Jenna McLaughlin, *FBI Kept Demanding Email Records Despite DOJ Saying It Needed a Warrant*, *The Intercept* (June 2, 2016), <http://bit.ly/1O6RKup>.

The Court should order the government to disclose whether it intends to use information obtained or derived from these or any other surreptitious surveillance

methods against Mr. Girgis. As discussed above, Mr. Girgis has a Fourth Amendment right to challenge any government searches conducted against him. He cannot, however, meaningfully challenge a search that he does not know even happened. And notice of these surveillance methods would obviously affect Mr. Girgis's forthcoming suppression motion, and is therefore required under *Brady*. See *Smith*, 904 F.2d at 965-66 (due process mandates the disclosure of information in the government's possession if nondisclosure would "affect[] the outcome of [a] suppression hearing").

Courts have long held notice to be a constitutionally required element of surreptitious searches, like wiretaps and sneak-and-peak entries. See, e.g., *United States v. Dalia*, 441 U.S. 238, 247-48 (1979) (observing that Title III provided a "*constitutionally adequate substitute for advance notice* by requiring that once the surveillance operation is completed the authorizing judge must cause notice to be served on those subjected to surveillance") (emphasis added); *Berger v. New York*, 388 U.S. 41, 60 (1967) (finding wiretapping statute unconstitutional because, among other things, it had "no requirement for notice as do conventional warrants"); *United States v. Freitas*, 800 F.2d 1451, 1456 (9th Cir. 1986) (finding sneak-and-peak warrant constitutionally defective for its failure to provide explicitly for notice within a reasonable time). And Congress has incorporated express notice provisions into many surveillance statutes, such as Title III, because it recognized that "all authorized interceptions must eventually become known at least to the subject" in order to "insure the community that the techniques are reasonably employed." *United States v. Donovan*, 429 U.S. 413, 438 (1977) (quoting

S. Rep. No. 1097, 90th Cong., 2d Sess., p. 2194 (1968)); *see also* 50 U.S.C. § 1806(c) (FISA electronic surveillance); *id.* § 1825(d) (FISA physical search); *id.* § 1842(c) (FISA pen register).

Courts can only confront the government’s use of various technologies to carry out surreptitious searches in criminal investigations if the government provides notice. The government, however, likely believes that notice is *not* required, given its past approach to such situations. *See, e.g.,* Charlie Savage, *Reagan-Era Order on Surveillance Violates Rights, Says Departing Aide*, N.Y. Times (Aug. 13, 2014), <http://nyti.ms/1wPw6l0> (describing the government’s view that “defendants have no right to know” if investigators derived evidence from an E.O. 12,333 intercept). But these programs present difficult and novel constitutional questions, and it is not the government’s prerogative to unilaterally conclude that its surveillance is legal or irrelevant. *See Alderman*, 394 U.S. at 183-84 (stressing the constitutional importance of adversarial procedures).

Moreover, notice is statutorily required under 18 U.S.C. § 3504. Under that statute, if a party in a proceeding before any court claims that “evidence is inadmissible” because “it is the primary product of an unlawful act or because it was obtained by the exploitation of any unlawful act” then the government must “affirm or deny the occurrence of the alleged unlawful act.” The statute defines “unlawful act” as “the use of any electronic, mechanical, or other device (as defined in section 2510(5) of this title)

in violation of the Constitution or laws of the United States or any regulation or standard promulgated pursuant thereto.” *Id.* § 3504(b).

A “cognizable claim” for notice under the statute “need be no more than a ‘mere assertion,’ provided that it is a positive statement that illegal surveillance has taken place.” *United States v. Apple*, 915 F.2d 899, 905 (4th Cir. 1990) (citing *United States v. Tucker*, 526 F.2d 279, 282 & n.4 (5th Cir. 1976)). The party must make a *prima facie* showing that he was “aggrieved by the surveillance”: “that [he] was a party to an intercepted communication, that the government’s efforts were directed at [him], or that the intercepted communications took place on [his] premises.” *Apple*, 915 F.2d at 905. Of course, because a defendant will have only limited information about the government’s undisclosed surveillance, this initial showing need not be complete; it must only have a “colorable basis.” *Id.* (citing *United States v. Pacella*, 622 F.2d 640, 643 (2d Cir. 1980)); *see also In re Grand Jury Matter*, 683 F.2d 66, 67 (3d Cir. 1982) (requiring notice under § 3504 upon the affidavits of the defendant and another individual that “there had been ‘unusual sounds’ on the defendant’s phone, ... and that two policemen had told the other individual that the appellant’s phone had been wiretapped”).

Mr. Girgis has made the requisite showing for notice under § 3504. Indeed, the sheer volume of communications the government intercepted from Mr. Girgis – including communications with individuals overseas – strongly indicate that the government utilized surveillance methods other than traditional FISA. Mr. Girgis’s international electronic communications and other online activities could readily have

been vacuumed up by the government's dragnet collection of content and metadata under E.O. 12,333, either through bulk surveillance or by targeting individuals overseas. Similarly, any electronic communications Mr. Girgis had with people located overseas were very likely intercepted under Section 702 of FISA. And other records related to Mr. Girgis's online communications and activities were also very likely initially obtained using national security letters.

But Mr. Girgis will never have an opportunity to test the legality of this surveillance and the extent to which the government relied on it to obtain or derive evidence against him without notice of the surveillance methods and legal authorities that the government actually employed and relied upon in its investigation. *See United States v. Alter*, 482 F.2d 1016, 1027 (9th Cir. 1973) (finding the government's response to a claim under § 3504 insufficient because it was conclusory, failed to clearly identify all governmental agencies involved in the surveillance, failed to identify the date ranges of the surveillance, and relied on vague hearsay recitations).

Finally, Fed. R. Crim. P. 16 also supports Mr. Girgis's request for notice. Such information is plainly necessary for the defense to prepare any motion to suppress as outlined above.

* * *

The Second Circuit has stressed the importance of adversary litigation to our system of justice: “[p]articularly where liberty is at stake, due process demands that the individual and the government each be afforded the opportunity not only to advance

their respective positions but to correct or contradict arguments or evidence offered by the other.” *United States v. Abubamra*, 389 F.3d 309, 322 (2d Cir. 2004). Here, the government is seeking to defeat Mr. Girgis’s due process rights and keep all information about the wide-ranging electronic surveillance it conducted of him secret, for all time. As such, Mr. Girgis cannot meaningfully prepare either a suppression motion or a trial defense, since the defense is being kept in the dark about information that is critical to advancing adversarial arguments.

Mr. Girgis was either the target of years of FISA surveillance, or his personal communications – including hundreds of calls and thousands of electronic messages – were intercepted incidentally to such surveillance. Moreover, Mr. Girgis may well have had his communications intercepted through other surreptitious methods, and the government likely relied on that surveillance to obtain or derive evidence against him. Mr. Girgis has a right to challenge the legality of any surreptitious surveillance and collection of his electronic communications and activities, and that cannot be effectuated without proper notice and access to the materials authorizing that surveillance. Consistent with statutory law and the Constitution, the Court should order disclosure of the FISA warrants, applications, and related materials, and notice of any other surveillance methods the government may have used.

II. Under Brady and Rule 16, the government must disclose information (1) material to Mr. Girgis’s *Franks* motion, (2) material to his *mens rea*-related defense, and (3) material to undermining the adequacy and good faith of the government’s investigation.

The defense served two discovery demands requesting (1) additional information about Special Agent Brian Connors’s misrepresentations and omissions in his warrant applications; (2) information about several Egyptian officials’ efforts to turn expatriates into unwitting intelligence assets; and (3) information about disgraced former FBI Special Agent in Charge Charles McGonigal’s involvement in the Girgis investigation. The government has refused to provide any of the requested materials. Since the requested information is plainly material to the defense, the Court should order disclosure under *Brady* and Federal Rule of Criminal Procedure 16.

Under *Brady*, 373 U.S. at 87, the government must disclose evidence in its possession that is favorable to the accused. This includes evidence material to guilt or punishment, and impeachment evidence. *Giglio v. United States*, 405 U.S. 150, 154 (1972). As the Supreme Court has explained, evidence is material when, taken as a whole, it could reasonably put the case “in a different light.” *Kyles v. Whitley*, 514 U.S. 419, 434-36 (1995). The *Brady* rule applies equally at the trial stage and at the suppression stage. *See Gamez-Orduno*, 235 F.3d at 461; *Smith*, 904 F.2d at 965-66 (5th Cir. 1990). Indeed, in keeping with the constitutional principles espoused in *Brady*, the Court has already ordered the government to immediately provide to Mr. Girgis any potential *Brady* or

Giglio material “promptly after its existence becomes known” and “sufficiently in advance of trial.”

Likewise, Fed. R. Crim. P. 16(a)(1)(e)(i) requires the government to disclose evidence that is “material to preparing the defense.” This materiality standard is not difficult to meet: evidence is material if it “could be used to counter the government’s case or to bolster a defense.” *United States v. Stevens*, 985 F.2d 1175, 1180 (2d Cir. 1993).

A. The government must provide further information about potential misrepresentations or omissions in the traditional search warrant application the government submitted.

Based on the information the defense currently possesses, Mr. Girgis’s case involves two different types of warrants. As detailed above, the government sought and obtained FISA warrants that it used to intercept Mr. Girgis’s communications. Separately, the government also obtained a traditional warrant to search Mr. Girgis’s person, electronic devices, luggage, personal effects, and the contents of his purported email and iCloud accounts. Ex. E. Like the FISA warrant applications, the traditional warrant application was sworn out by Connors. And like the FISA warrants, Mr. Girgis intends to file a motion to suppress the traditional warrant on *Franks* grounds, given Connors’s misrepresentations and omissions about [REDACTED] criminal record and credibility issues.⁶ Indeed, as detailed above, it appears that the materiality of Connors’s

⁶ A full accounting of the facts surrounding Connors’s omissions about [REDACTED] criminal record was provided earlier. *Supra* Pt. I.

misrepresentations and omissions was the subject of an internal government investigation. Ex. C.

With regard to the traditional warrant, as with the FISA warrants detailed above, both *Brady* and Fed. R. Crim. P. 16 mandate that the government disclose any information in its possession about Connors's misstatements or omissions – particularly the investigation that resulted in the government's unilateral determination that they were not “material.” Not only is this information textbook *Giglio* material, but it has the potential to affect the outcome of Mr. Girgis's forthcoming *Frankes* motion.

The government, however, has refused to disclose any further information aside from that contained in its initial *Brady* disclosure. In fact, the government has not even specifically identified what the “misrepresentation/omission” referenced in the June 2020 email was, and whether it referred to Connors's failure to disclose [REDACTED] criminal record or something else entirely. Instead, the government has chosen instead to rely on the FBI's own internal determination that the misstatement or omission – whatever it may have been – did not rise to the level of a *Frankes* violation. But the ultimate determination of that question is up to the Court, not the government. In order to effectively raise a *Frankes* claim, the defense is entitled to all information in the government's possession related Connors's misstatement or omission – including identifying what it was, and disclosing any documents or information about the government's investigation into it. *See Biles v. United States*, 101 A.3d 1012, 1020 (D.C. 2014) (“the suppression of material information can violate due process under *Brady* if

it affects the success of a defendant's pretrial suppression motion") (citing *Gamez-Orduno*, 235 F.3d at 461).

Accordingly, pursuant to *Brady* and Fed. R. Crim. P. 16, the Court should order the government to disclose any information in its possession regarding the misstatement or omission referenced in Connors's June 23, 2020, email.

B. The government must provide information and unredacted reports about the efforts of nine Egyptian officials to turn expatriates into unwitting intelligence assets.

The government alleges that Mr. Girgis acted as an unregistered agent of the Egyptian government. In the discovery the government has provided, nine Egyptians appear repeatedly in FBI reports and intercepted communications:

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

[REDACTED] are specifically identified as subjects of an "FBI assessment." And [REDACTED] are named as individuals responsible for "tasking" Mr. Girgis to conduct influence operations. Yet, where these individuals are involved, the FBI reports the government provided were heavily redacted.

In its discovery demand, the defense requested that the government disclose: unredacted FBI reports detailing the relationship between Mr. Girgis and [REDACTED]; an unredacted FBI report outlining details of [REDACTED] involvement in a trip to Egypt that Mr. Girgis allegedly organized; unredacted confidential human source reports and electronic communications containing information about the above-mentioned individuals; and any information in the government's possession that the nine Egyptians were involved in a campaign to "turn" expatriates into unwitting stooges. Ex. D. As the defense subsequently explained to the government, Mr. Girgis has been preparing a defense that these individuals cultivated him as an unwitting asset. As a result, information that the nine Egyptians had engaged in an effort to turn expatriates into unwitting intelligence assets is material to the investigation and preparation of the defense. Ex. G.

The defense's discovery request was narrowly tailored to the precise information needed for Mr. Girgis to effectively prepare his defense. The nine named Egyptians were individuals whom the government specifically identified as being closely involved in the allegations against Mr. Girgis. Indeed, two were identified as people responsible for "tasking" Mr. Girgis, and the others appear repeatedly in FBI reports and intercepted communications as individuals attempting to cultivate Mr. Girgis as an asset.

The government has nevertheless refused to provide the requested information and unredacted reports, insisting that it is not discoverable because it is "irrelevant" to

the elements of the charged crimes. But the government is mistaken. While the *mens rea* required under 18 U.S.C. § 951 has been the subject of debate – and will undoubtedly be a litigated issue in this case – at minimum, the government must prove that Mr. Girgis knowingly acted as a foreign agent. *See United States v. Duran*, 596 F.3d 1283, 1296 (11th Cir. 2010). To that end, a viable defense is that Mr. Girgis did not knowingly act as a foreign agent, but instead had been the target of an effort to “turn” him into an unwitting stooge of the Egyptian government – a defense that goes directly to the knowledge element of 18 U.S.C. § 951. Therefore, information in the government’s possession regarding the efforts of the nine Egyptians to turn expatriates into unwitting assets is material to both guilt and punishment, and therefore plainly discoverable under both *Brady* and Fed. R. Crim. P. 16.

Accordingly, the Court should order the government to disclose all information in its possession regarding the efforts of the nine Egyptians to cultivate unwitting intelligence assets in the United States. The Court should also order disclosure of unredacted copies of the reports cited in Requests 1a and 1c-e of the defense’s discovery request. Ex. D.⁷

⁷The defense also requested several other unredacted reports concerning the Girgis investigation. Ex. D [Requests 1f-1i]. To the extent these documents contain material information about the nine Egyptians or any efforts to cultivate unwitting intelligence assets in the United States, these reports should be ordered disclosed, as well.

C. The Court should order disclosure of information about the role Charles McGonigal played in the Girgis investigation.

Finally, the Court should order the government to disclose any information in its possession about the role disgraced former FBI Special Agent in Charge Charles McGonigal played in the Girgis investigation. This information – which goes directly to the integrity of the FBI’s investigation and the credibility of its sources – is discoverable under *Brady*, *Giglio*, and Fed. R. Crim. P. 16.

The charges against Mr. Girgis stem from an investigation by the FBI’s New York Counterintelligence Division. During that investigation, which began as early as 2016, the FBI obtained information from confidential human sources, at least one of whom [REDACTED]. Ex. F. From the beginning of the Girgis investigation until 2018, the FBI’s New York Counterintelligence Division was run by Special Agent in Charge Charles McGonigal.

In January 2023, the Department of Justice unsealed two indictments against McGonigal. The first, filed in the Southern District of New York, accused McGonigal of accepting concealed payments and conspiring to help Russian oligarch Oleg Deripaska evade sanctions. According to SDNY prosecutors, McGonigal cultivated a relationship with a representative of Deripaska while serving as Special Agent in Charge, helped that representative’s daughter obtain a job with the NYPD, and, after retiring

from the FBI, conducted an investigation into one of Deripaska's rival oligarchs. Ex. J.

Meanwhile, federal prosecutors in the District of Columbia accused McGonigal of accepting concealed payments, while still Special Agent in Charge, from a former Albanian intelligence official with ties to the Albanian Prime Minister. Among other misconduct, McGonigal opened an investigation into a U.S. citizen lobbyist who belonged to a rival political party of the Prime Minister, and used the former Albanian intelligence official as a confidential human source in that investigation. Ex. K.

According to press reports, the charges against McGonigal “set off a scramble within the [FBI] to assess the potential damage and determine whether any counterintelligence or law enforcement operations were compromised,” with the FBI director “treating the case as a top priority.” Michael Rothfeld et. al, *How Prosecutors Say a Top FBI Agent Sold His Services Overseas*, N.Y. Times (Feb. 3, 2023), *available at* <https://www.nytimes.com/2023/02/03/nyregion/fbi-intelligence-charged-albania.html>. The FBI's damage assessment “likely is looking back much further” than 2017, and concerns have been raised “about the breadth and duration of his possible deceptions.” *Id.* As one former FBI official put it, “It puts a question mark next to everything he was involved in.” *Id.*

Upon learning of the charges against McGonigal and the FBI's ongoing damage assessment, the defense sent a discovery demand to the government requesting any and all information regarding McGonigal's involvement in the Girgis investigation,

including information regarding (1) whether McGonigal oversaw or was involved in any part of the investigation into Mr. Girgis, (2) authorized any steps in that investigation, and/or (3) approved any classified FISA warrant applications. Ex. G, Ex. I. The government, however, has taken the position that information about McGonigal's involvement in the Girgis investigation is "irrelevant." The government is wrong: the information sought is indisputably material under *Brady* and Fed. R. Crim. P. 16.

The defense is entitled to any information that provides a basis to attack the reliability, thoroughness, and good faith of the government's investigation. *See Kyles*, 514 U.S. at 420; *see also Nuckols v. Gibson*, 233 F.3d 1261, 1266-67 (10th Cir. 2000) (finding a *Brady* violation where the "prosecution withheld evidence that would have allowed defense counsel the means to test [the police officer's] credibility"). Here, McGonigal was the Special Agent in Charge of the FBI division that investigated Mr. Girgis. At the time he was Special Agent in Charge, McGonigal was concealing his relationships with foreign intelligence and governmental officials, accepting concealed payments, and instigating investigations of the foreign agents' and officials' political rivals. Indeed, as charged in the District of Columbia indictment, McGonigal even used one of the former foreign intelligence agents with whom he conspired as a confidential human source in an investigation into a U.S. citizen.

The parallels with the Girgis investigation are stark. During the time McGonigal was Special Agent in Charge, the FBI investigated Mr. Girgis, a United States citizen, as a potential foreign asset. The Girgis investigation involved a confidential human

source [REDACTED], and revealed deep schisms in that community between two rival groups: the Muslim Brotherhood and the Coptic Christians. Throughout the Girgis investigation, at least one confidential human source – [REDACTED] – was grossly mishandled, with the lead investigator, Connors, conspicuously failing to conduct a basic background check, include information about [REDACTED] criminal record in warrant applications, or even officially sign him up as a source before “tasking” him. The use of foreign sources, the involvement in squabbles between rival political groups, and the curious failure to follow basic investigatory protocols, all starkly parallel the irregularities that characterized McGonigal’s charged misconduct.

Since the nature and extent of McGonigal’s involvement casts doubt on the integrity of the government’s investigation and the credibility of the it witnesses, it is *Brady* material that could reasonably cast the entire case in a different light. *Kyles*, 514 U.S. at 434-36. And any documents regarding the FBI’s damage assessment as they potentially relate to the Girgis investigation would be material to the defense and thus discoverable under Fed. R. Crim. P. 16(e). Indeed, since the search warrants in this case may have been obtained by relying on sources that had compromised relationships with McGonigal, information about McGonigal’s role is material not only to Mr. Girgis’s trial defense but also to his forthcoming suppression motions. As such, the information the defense has sought regarding McGonigal’s role in the Girgis investigation is plainly discoverable.

Therefore, the Court should order the government to disclose any and all information regarding McGonigal's involvement in the Girgis investigation, including information regarding whether McGonigal oversaw or was involved in any part of the investigation into Mr. Girgis, authorized any steps in that investigation, and/or approved any classified FISA warrant applications. The Court should further order disclosure of any documents regarding the FBI's damage assessment into McGonigal as they potentially relate to the Girgis investigation.

CONCLUSION

The Court should order the government to disclose: (1) the FISA warrants, applications, and underlying materials, and notice of any other surreptitious surveillance the government conducted; (2) information about Connors's potentially material misrepresentation or omission in his warrant applications; (3) information about the nine named Egyptian officials and their efforts to cultivate unwitting assets in the United States; and (4) information about the role Charles McGonigal played in the Girgis investigation.

Dated: April 28, 2023
New York, New York

Respectfully submitted,

_____/s/_____

Andrew John Dalack, Esq.
Hannah McCrea, Esq.
Michael Arthus, Esq.
Federal Defenders of New York
52 Duane Street, 10th Floor
New York, NY 10038
(212) 417-8700